セキュリティポリシー策定・運用支援
ナレッジマネジメントシステムの開発

川西　宏昌、大田　俊介、三代　尚志、坂井　司、田中　保彦
株式会社 日本総合研究所　セキュリティ事業推進部

本技術開発は、セキュリティポリシー策定を支援する「セキュリティポリシー策定・運用支援ナレッジマネジメントシステム」の構築を目的としている。本システムは、電子政府の情報セキュリティを確保するにあたっての基本方針となるセキュリティポリシーの策定に係る作業負荷を軽減するために、ナレッジマネジメントの手法を利用するものである。本システムによってセキュリティポリシー策定・運用に関する作業を支援することが可能となる。本技術開発は、初年度を調査・設計、次年度を実装および検証実験とする 2 ヵ年計画で実施されたものである。本報告では、最終年度に当たる平成 13 年度に行った具体的な作業内容ならびに成果について報告する。

1 はじめに

政府は、2003 年度までに行政の効率化や国民負担の軽減を目標に行政手続きを電子化する電子政府の基盤を構築することを目指している。

電子政府の構築は、デジタル経済・社会の一つのモデルであり、その中で実施される情報セキュリティ確保のための対策もまた、広く民間の範となるものである。それによって、我が国のネットワーク全体の安全性・信頼性を高めることが可能となる。更に、具体的に進みつつある海外の同様の取り組みと連携していくことにより国際的な貢献につながることも期待される。このため、電子政府の構築に向けて、情報セキュリティ政策を重要なものとして位置づけ、積極的な貢献を行っていく必要がある。

本技術開発は、電子政府の推進において情報セキュリティ面がその制約要因とならないよう、電子政府における情報セキュリティ確保のための基盤技術の開発を行うことを目的として、平成 12 年 4 月に通商産業省（現経済産業省）が策定した「情報セキュリティ政策実行プログラム～電子政府のセキュアな基盤構築に向けての通商産業省の貢献～」の重要な一部として実施されたものである。

実際に適用される情報セキュリティ対策の基本方針を定めるものとしてセキュリティポリシーがある。セキュリティポリシーは、対象となる検討範囲が多岐に及ぶことから、策定にあたって多くの労力を必要としているのが現状である。

一方、セキュリティポリシーの策定は、情報技術を安全に活用するための必須要件とされており、セキュリティポリシー策定作業に関する負荷を軽減することが強く要求されている。

セキュリティポリシー策定の作業負荷を軽減するためには、セキュリティポリシー策定に関する各種のノウハウを知識ベースとして保有し、電子政府の情報セキュリティ面を支える各拠点の担当者を支援するための情報システムが有用であると考えられる。

2 技術開発の目標と内容

2.1 技術開発の目標

「セキュリティポリシー（関連規程・文書）策定」及び「個別のセキュリティ対策」は、専門家の知識・ノウハウに依存してそれぞれ行われているケースが多い。情報セキュリティ対策の立案に際しては、検討対象となる範囲が広く、当該分野の専門家の支援無しでは、実効性を伴うセキュリティポリシーを策定することは事実上困難であると考えられる。

本技術開発では、電子政府においてセキュリティポリシー策定に携わる担当者が、自組織における環境要因・制約要因などの情報を入力することにより、情報セキュリティ対策の方針を示す「セキュリティポリシー文書」を自動生成することを目標としている。これにより担当者は、本技術開発によるナレッジマネジメントシステムに対して、画面を通じたインターフェイスによる質問項目に回答することで、自組織の要因を加味したセキュリティポリシー文書を策定することが可能となる。

2.2 技術開発の内容

上記目標を達成するにあたっては、セキュリティポリシーそのものに関する策定・体系化作業、当該セキ

ュリティポリシーを生成するための情報システムが必要となる。

以下、各項目における技術開発内容について記す。

(1) セキュリティポリシー雛形の策定

セキュリティポリシー文書の策定にあたっては、次の２つのアプローチが考えられる。それは、①各脅威への対応に基づき対策基準を逐一設定し、これらを統合することで文書化するアプローチと、②標準的な文書を定めておき、これらに対して諸処の要因に基づく変更箇所へのカスタマイズを加えるアプローチである。前者①は、各脅威への仔細な対応が可能となるが、個々の基準を積み上げることでセキュリティポリシー文書・規程体系を構成することとなるために、体系にまとまりを欠く。一方、後者②は、前者①に比べ、セキュリティポリシー策定に必要な論点を整理・分類することで、体系化されたセキュリティポリシー文書を効率良く作成することが可能である。本技術開発においては、体系的であることを重視し、後者②のアプローチを採用した。

本技術開発においては、前記②のアプローチでの元となる文書である「情報セキュリティポリシーに関するガイドライン」（平成 12 年 7 月 18 日、情報セキュリティ対策推進会議決定）により示される内容をもとに、各種の関連文書からの知見やノウハウを盛り込み、電子政府向けの「セキュリティポリシー雛形」を新たに策定した。本雛形は、セキュリティポリシーの一例として、そのまま活用し得る形態となっている。

また、セキュリティポリシーの実効性を高めるためには、セキュリティポリシー策定主体となる各組織における環境要因・制約要因を加味することが必要となる。実際のセキュリティポリシーでは、各組織の諸条件を加味した上で、あるべき姿に若干のカスタマイズを施すことが多い。そこで、本技術開発においても、策定組織において発生することが想定される条件を抽出し、これらの条件に該当する場合に、如何に雛形文書に改訂が施されるか、という観点で、判断基準の整理を行った。これを、セキュリティポリシーの策定に際しての「論点集」としてまとめた。

(2) ナレッジマネジメントシステムの開発

セキュリティポリシー策定を支援するナレッジマネジメントシステムは、その機能を以下のように分類出来る。

ナレッジマネジメントシステムの機能分類

1）エキスパート機能
2）文書生成機能
3）文書管理機能

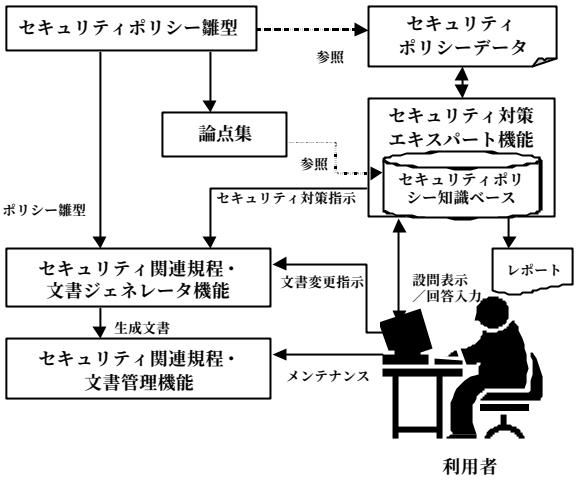

図１：機能間関連図

本システムが起動すると、まず、1）のエキスパート機能が呼び出され、画面インターフェイスを通じて策定主体の諸条件入力を促す。そして、ここで入力された情報を入力パラメータとして、エキスパートシステムが稼動する。このときエキスパートシステムが稼動する際に適用される知識ベースは、セキュリティポリシー雛形とともに策定された「論点集」が用いられる。「論点集」を知識処理形式に表現しなおして知識ベースとして格納することにより、入力パラメータに応じたルールが適用され、セキュリティポリシー雛形に対して、如何なるカスタマイズを施せばよいかという指針が導出される。

こうして導出された指針をもとに、セキュリティポリシー雛形に対して実際にカスタマイズ処理を施すのが、2）の文書生成機能である。

指針の内容によっては、セキュリティポリシーを構成する 1 ブロックをすべて削除する、あるいは末尾の表現を修正するなど、個々の内容に応じた適切な処置を施さねばならない。そこで、文書生成機能は、元となるセキュリティポリシー雛形文書を、情報システムでカスタマイズ可能なように、詳細ブロックに分割し、指針に従ったセキュリティポリシー文書として再構成する機能を担う。

また、セキュリティポリシー文書は、電子政府を対象として策定された一例である雛形をベースとしている。そのために、広域の電子政府（電子自治体を含む）までも対象として適用する場合には、役職

名や組織名、または情報の伝達にかかわる諸機能などについて、自組織にあった適切な表現に変更しておく必要がある。このような処理を機械的に行うのが、3）の文書管理機能である。文書管理機能では、当該セキュリティポリシーの改版履歴などを管理する機能も併せ持つことで、組織内での担当者変更が発生した場合などにも、運用面でのセキュリティポリシーの有効性劣化を防ぐことが可能となる。

なお、これらの情報システムによる機能の実現にあたっては、開発期間の短期化を企図し、既存のエキスパートシステム作成支援ツールや、文書管理ツールの活用を行うこととした。エキスパートシステムとしては昨年度の調査によって KBMS を利用することとした。文書管理システムについては、コストと機能の兼合いから既存の文書管理ツールは用いず、今年度独自に実装することとした。

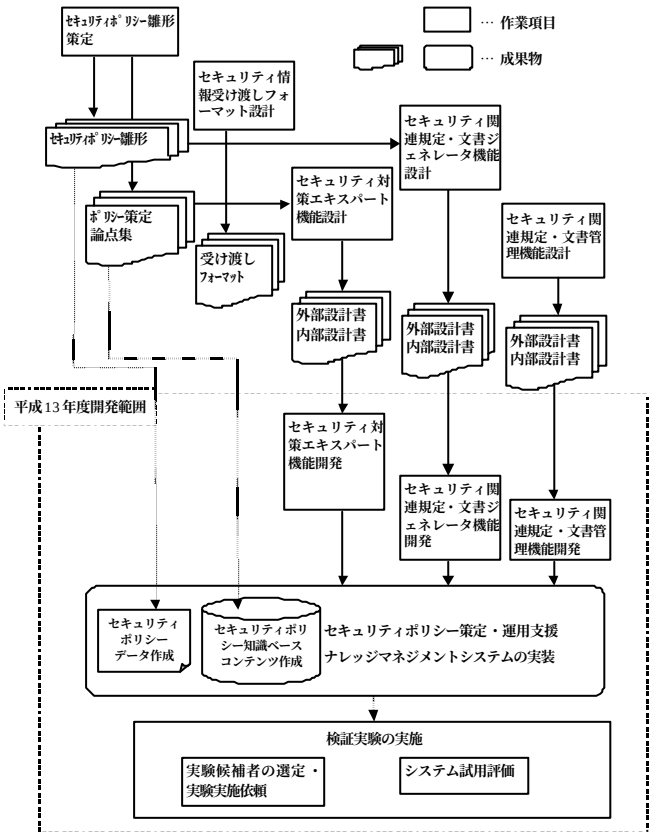

図 2：本技術開発の全体像

3 本年度の活動状況

3.1 ナレッジマネジメントシステムの実装

本年度は、昨年度の設計をベースにエキスパート機能、文書ジェネレータ機能、文書管理機能、ルールメンテナンス機能の４つの機能実装を行った。（ルールメンテナンス機能は設計上はエキスパート機能の一部である。）

(1) エキスパート機能

本機能は、知識ベースに定義されたルールに従って、ユーザに制約条件などの入力を促す GUI を表示し、ユーザに入力・選択された値に応じて推論を実行する。エキスパート機能では、昨年度の成果である「論点集」をエキスパートの知識ベースとして実装する。「論点集」は、策定組織において発生することが想定される条件を抽出し、これらの条件に該当する場合に、如何に雛型のポリシー文書に反映するかを定義したルールであり、268 の論点から成る。エキスパート機能では、ルールとフレームという２つの知識表現を用いて「論点集」を定義する。ルールとフレームは今回採用したエキスパートシステム KBMS の知識表現のフレームワークである。以下フレームとルールについて説明する。

・フレーム

フレームとは推論過程における結果や推論時に必要な知識を定義したものである。フレームはオブジェクト指向のクラスとインスタンスと同じ概念を持っており、各フレームは共通のクラスから生成される。今回以下のようなクラスを用意し、このクラスのインスタンスとしてフレームを定義した。

```
(defFrame 論点
        (ルール番号      0      (:vtype long) )
        (推論結果        nil    (:vtype symbol) )
        (入力値          nil    (:vtype symbol) )
        (変更指示リスト ()      (:vtype msymbol) )
)
```

上記の例では ”論点” という名前のクラスを作成し、４つの値をフレームが持つことを定義している。各値は名前と初期値、値の型によって定義される。このクラスから、各ルールの結果を格納するためのフレームが生成される。「論点集」を知識ベースに定義するために各論点に対応するフレームを用意する。

・ルール

ルールは推論を実行するものであり、上記で定義したフレームの内容を参照・修正しながら推論を行う。ルールとしては前向き、後ろ向き、仮説推論などさまざまなルールを記述することができるが、今回の論点

集を実装するにあたっては前向き推論のみを利用した。

下記のルールは、「もし質問 1 の回答が "no" ならば、ポリシー文書の [1:2:1:2:0:7] の部分を "情報システム" という語で置換えなさい。」というルールを定義したものである。

```
(defRule  論点集 論点ルール 1 :priority 10
  (frame ?frm&(instance_of 論点) (ルール番号 1)
  (推論結果 nil) )
→
  (bind ?answer {questionYN(1); } )
  (modifyFrame ?frm (推論結果 ?answer) )
)
(defRule 論点集 論点ルール 2 :priority 12
  (frame ?frm&(instance_of 論点) (ルール番号 1)
  (推論結果 no)
→
  (bind ?res {action(?frm @単語置換,
            @[1:2:1:2:0:7], @情報システム);} )
)
```

"questionYN" によって GUI 上に質問内容を示した Yes/No を選択させる質問画面が表示される。その結果は "modifyframe" を通じて対応するフレームに格納される。"論点ルール 2" では、"論点ルール 1" の結果を参照し、"no" だった場合は、"action" を通じて変更指示内容が対応するフレームの変更指示リストに追加される。

このフレームとルールを用いて推論を実行する。実行結果は全てフレームに保存されているため、フレームの変更指示リストに格納されている変更指示パラメータをまとめ、文書ジェネレータ機能に引き渡すことで、推論結果に従ったポリシー文書の作成を依頼することが可能となる。

(2) 文書ジェネレータ機能

文書ジェネレータ機能は、作成された変更指示パラメータを受け取り、セキュリティポリシー文書の雛型を修正しながら、適切なセキュリティポリシー文書の作成を行う。本機能は SGML をベースに構築している。ここで SGML を利用する理由は２つある。１つは文書のスタイルを本文と別に設定することができる点である。これによりセキュリティポリシー文書のスタイルを柔軟に変更可能となる。２つめは SGML により多様なフォーマットのドキュメントへの変換が可能となる点である。現在のシステムでは Word 形式の文書が出力されるようになっているが、HTML や XML、TeX などの文書へ変換可能である。

文書ジェネレータでは、セキュリティポリシー文書の雛型を以下のように文書の構造をインデックス化したファイルとして保持している。

```
0,0001,0000,0000,0000,0000,0000,0, 電子化情報管理
0,0001,0000,0000,0000,0000,0001,0, 基準
0,0001,0001,0000,0000,0000,0000,0, 目的
   …
0,0001,0003,0003,0001,0000,0022,0, 論ずる。
```

このインデックス化されたセキュリティポリシー文書の雛型にエキスパート機能で指定された操作を加えていく。文書ジェネレータ機能がサポートする変更指示の記述には以下の 6 つがある。

変更指示	インデックス指定	変更値
単語削除	[1:1:1:1:1]	―
単語置換	[1:1:1:1:1]	単語
範囲削除	[1:1:1:1:1-3]	―
範囲置換	[1:1:1:1:1-3]	文字列
行削除	[1:1:1:1:0]	―
行置換	[1:1:1:1:0]	行

これらの変更指示を解釈し、セキュリティポリシー文書を変更して SGML のソースファイルを自動生成する。生成した SGML のソースファイルとスタイルファイルをコンパイルして Word 形式のドキュメントを作成する。スタイルファイルを変更することで自由にポリシー文書の体裁を修正することができる。セキュリティポリシー文書に対する変更は、システム上で図 3 の画面を通じて確認可能である。

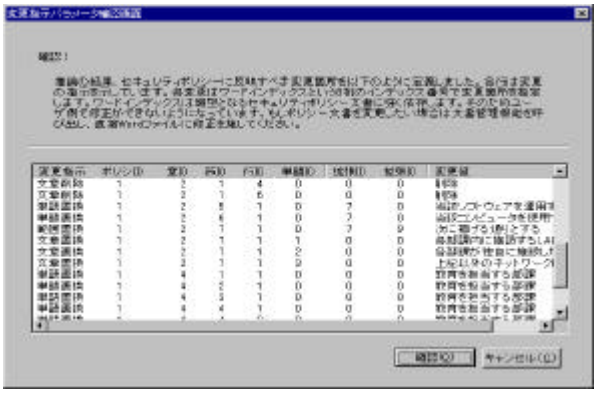

図 3：変更確認画面

(3) 文書管理機能

文書管理機能では、本システムにより生成される文

書に対して行うさまざまな操作・管理のための機能を提供する。具体的には以下の２つの機能を提供する。

・構成要素定義・管理機能

本機能では「構成要素」を単位とした、セキュリティポリシー文書に対する改版管理をサポートする。「構成要素」とは以下の 3 つによって構成されるもので、セキュリティポリシー文書中で単語（又はセンテンス）をどのように修正するかを定義したものである。

- 構成変数：文書中の単語（センテンス）
- 構成要素：構成変数を置換える語句
- コメント：変更の主旨

変更箇所を上記のような構成要素として管理することで、セキュリティポリシー文書に対する修正を機能的に管理可能となる。構成要素の定義は、システム上では図４の画面を通じて行われる。

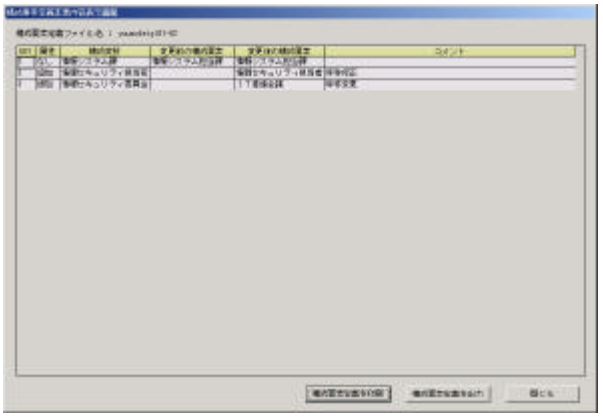

図 4：構成変数入力画面

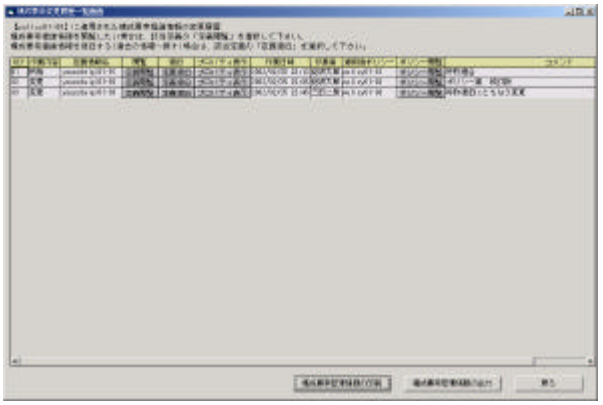

図 5：構成履歴管理画面

これらの構成要素は図 5 で示すように履歴管理されており、これにより文書の版管理を実現している。どの構成要素を原版のセキュリティポリシー文書に適用するかによって、出力される文書を変更することが可能である。例えば組織変更等が頻繁にある場合は、組織名やその関連項目を構成要素として定義しておき、それを適用することで最適なセキュリティポリシー文書を得ることができる。また、構成要素による変更を図 6 に示す画面を通じて確認することができる。

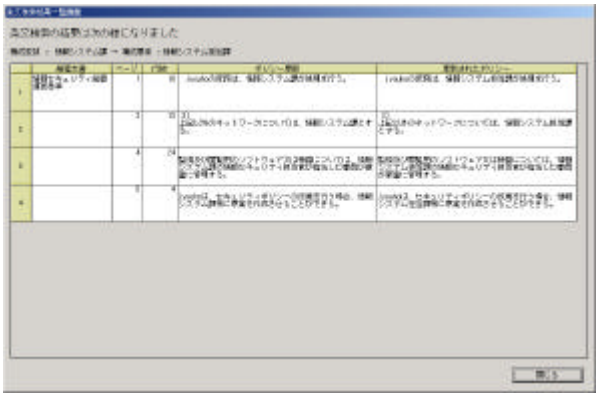

図 6：変更条文検索結果画面

・ポリシー文書出力機能

本機能は、構成要素が適用され変更されたセキュリティポリシー文書を外部ファイル、外部プリンタ、画面のそれぞれに出力する機能である。

(4) ルールメンテナンス機能

本機能は、(1)のエキスパート機能で利用されるルール及びフレームを動的に変更するものである。本システムではルールやフレームは知識ベースファイルに保存されている。このファイルから推論開始時に知識が読み込まれる。ルールメンテナンス機能はこの知識ベースファイル編集のためのエディタとして機能する。

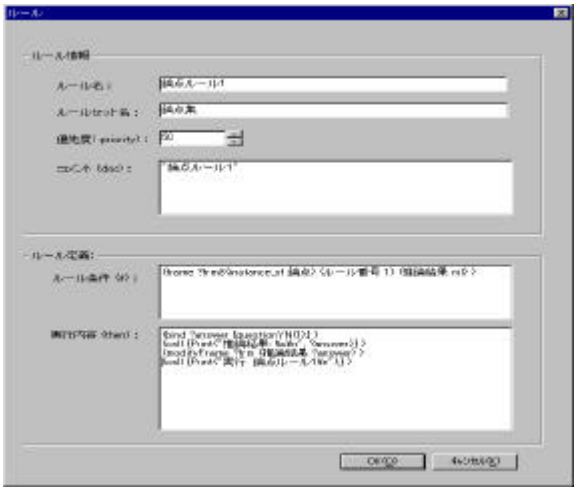

図 7：ルールメンテナンス画面

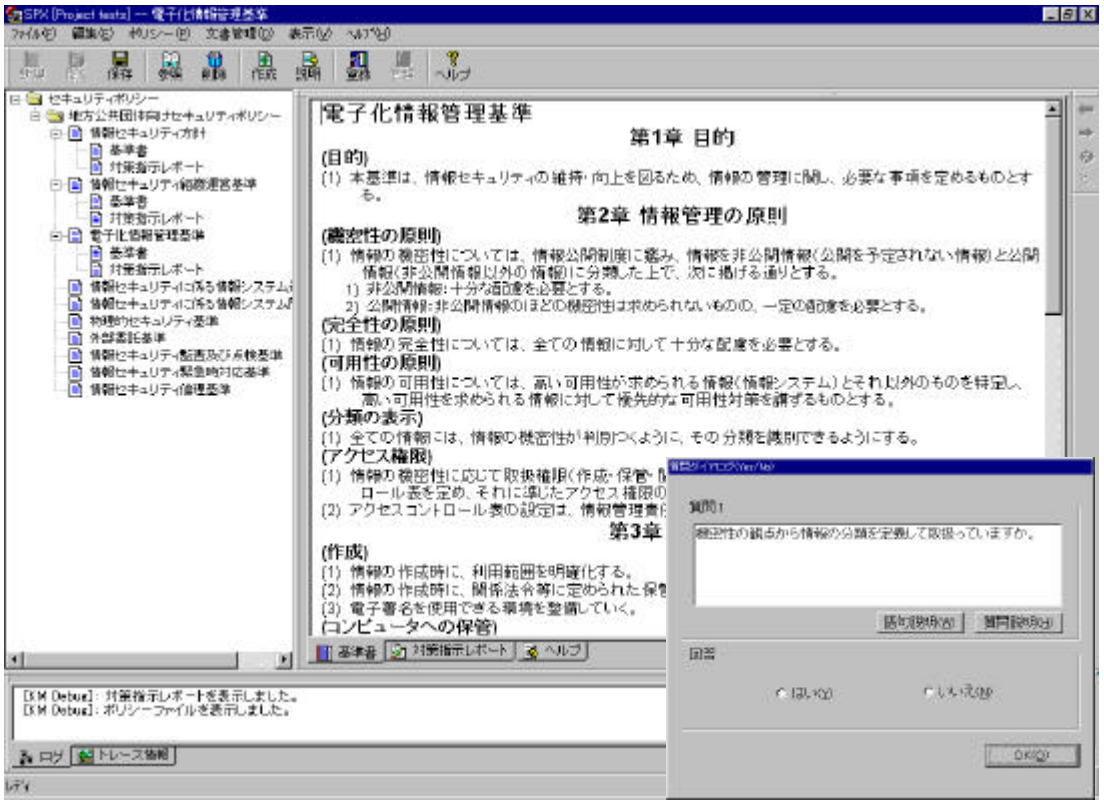

図 8：システムメイン画面

前述の 4 機能によって本システムは構成される。エキスパート機能、文書ジェネレータ機能、ルールメンテナンス機能は VC++にて実装した。これらの機能は約 60 程度のクラスで定義されている。SGML モジュールには OpenJade というオープンソースを利用した。文書管理機能は VB にて実装した。これらの機能は図 8 に示すようなメイン画面上で提供され、ユーザにセキュリティポリシー文書の表示やセキュリティポリシー策定をわかりやすい GUI にて表示する。

3.2 検証実験

本システムの、電子政府におけるセキュリティポリシー文書の策定・運用における有効性を検証するため、以下の検証項目について検証実験を行った。

- 本システムより出力されるセキュリティポリシー文書の妥当性
- セキュリティポリシー運用支援に関する機能の妥当性

(1) 検証実験の概要

広域の電子政府には電子自治体を含むものとして、地方公共団体において実際に情報資産の企画・運用・管理に携わる職員に対して、検証実験の協力を依頼し、５地点の団体（実験協力者７名）から協力を得た。

検証実験の実施方法として、セキュリティポリシー文書策定機能（エキスパート機能・文書ジェネレータ機能）については、実験協力者により実際に本システムの試用を行い、セキュリティポリシー文書の策定を行った。また、セキュリティポリシー運用支援機能（文書管理機能）については、本システムの画面上での操作説明及び機能説明を行った。実験協力者による本システムの試用ならびに出力されたセキュリティポリシー文書のレビューを通じて、検証項目に関する評価コメントをヒアリング及びアンケートにより実験協力者から収集した。

(2) 検証実験の結果

収集した評価コメントに基づき、本システムの検証を行った。

本システムより出力されるセキュリティポリシー文書については、電子政府として目指すべきセキュリティ目標として相応しく、実験協力者の所属団体のセキュリティ方針と照らしても適合性があり、また実現可能な内容となっていることが確認された。実験協力者が入力した判断基準（環境要因・制約要因等）に応じて知識ベースが処理するルールの妥当性が確認され、電子政府を目指す団体におけるセキュリティポリシー策定を支援できることが検証された。

セキュリティポリシー運用支援に関する機能については、組織体制の変更があった場合でも全てのセキュ

リティポリシー文書の整合性を確保した構成要素の変更が可能な点、地方公共団体ごとの独自な文書表現に対しても文書メンテナンスにより対応可能な点、及びセキュリティ対策を担当する職員の異動・引継ぎ等に対してセキュリティポリシー文書の改版履歴管理が有効である点等の評価を受けた。本機能の妥当性が確認され、セキュリティポリシー文書の運用を支援できることが検証された。

なお、評価コメントにおいて本システムをより良いシステムにするための意見に関しては、将来の本システムの発展のための課題として整理・確認する一方、本技術開発の範囲において対応可能なものに対しては検証実験終了後に本システムへの反映・実装を行った。

4 成果物

本年度の活動成果としては、以下に掲げる成果物が生成された。

・ナレッジマネージメントシステム（ソースプログラム・ロードモジュール）

下記の 10 文書に関する知識ベースがサポートされている。

①情報セキュリティ基本方針
②情報セキュリティ組織運営基準
③電子化情報管理基準
④情報セキュリティに係る情報システム運用基準
⑤情報セキュリティに係る情報システム開発基準
⑥物理的セキュリティ基準
⑦外部委託基準
⑧情報セキュリティ監査及び点検基準
⑨情報セキュリティ緊急時対応基準
⑩情報セキュリティ倫理基準

・取扱説明書

インストールマニュアル、ユーザマニュアル、管理者マニュアルの 3 つのマニュアルで構成される。

・試験成績書
・内部設計書（改訂版）

昨年度の成果である 3 つの内部設計書の内容を見直し、改訂を行った。

・開発成果報告書
・検証実験報告書

５地点の地方公共団体の協力を得て実施した検証実験の結果報告書。システム面及びセキュリティポリシー文書のコンテンツ面の 2 面から本システムの有効性・妥当性について検証した。

5 今後の課題

5.1 知識ベースメンテナンス機能

本年度構築したナレッジマネジメントシステムにおいては、知識ベースメンテナンス機能は、セキュリティポリシー文書の構成やエキスパート言語の仕様を知らなければ、簡単に修正を施すことはできない。というのも当初本機能は管理者のための機能として位置付けられていたためである。その一方、検証実験等を通じて、外部要因（国の「情報セキュリティポリシーに関するガイドライン」の改訂時におけるルールの見直し等）や内部要因（各組織でのセキュリティポリシーの策定・運用過程で抽出された新規ルールの追加や既存ルールの修正対応等）により、知識ベースそのものを変更することができないかというコメントを頂いた。本システムはセキュリティポリシー策定を支援することに主に焦点を当てたが、このようなニーズに対応するためには、ルールのメンテナンスをユーザレベルで行うための高度な GUI を備えた知識ベースエディタが必要となる。このようなエディタの整備によってユーザレベルでも柔軟にルールの変更が可能となり、本システムの拡張性を高めることができる。

5.2 セキュリティポリシーの複数類型化

本システムで用いるセキュリティポリシー雛形は、「情報セキュリティポリシーに関するガイドライン」をベースとして一通りの論点を洗出して策定されたものとなっている。しかし実際に、広域の電子政府（電子自治体を含む）での活用を想定した場合には、中央省庁と都道府県・市区町村での諸条件の違い（組織規模による情報システム運営体制の違い）や準拠するガイドラインの違い（「地方公共団体における情報セキュリティポリシーの例示」（平成 13 年 6 月）への対応）など、セキュリティポリシー策定にあたっての基本要件が類型化出来ることも考えられる。このような場合、類型要件に応じた複数の雛形を用意しておくことで、その後の論点整理についても、より効率的な処理を行える可能性が考えられる。

5.3 下位層への連携

本システムは、セキュリティポリシー策定を支援することにフォーカスを当てているが、その下位層に位置する情報セキュリティ実施手順等においては、昨年度、情報の自動収集を企図し、情報共通項目の定義を実施したにとどまった。今後、策定したセキュリティポリシー文書と関連して個別の情報システムのセットアップ方針を提示する機能が備われば、より効果的に

各組織のセキュリティ確保に資するものと考えられる。

6 まとめ

本年度は、昨年度実施したセキュリティポリシー雛型・論点集をベースに、セキュリティポリシーエキスパートシステムの開発を行った。さらに作成したシステムを用いて検証実験を行い、その評価を行った。検証実験を通じて本システムの有用性・妥当性を検証することができ、各実験協力者からはリリースされれば使用したいシステムであるとの評価を受けた。

本システムは、単に昨年度作成したセキュリティポリシー文書の策定だけではなく、広く一般的なセキュリティポリシー文書をエキスパート機能を利用して自動生成するための枠組みを提供する。本枠組みを利用して電子政府向けのセキュリティポリシー文書作成のための知識ベースを提供したことで、これまで手作業で行ってきた作業を効率化できるほか、セキュリティポリシー策定に関するさまざまな情報を本システムを通じて参照可能である。また本システムではセキュリティポリシー策定後の運用を含めた作業も支援することにより、担当者の負荷を軽減することが可能である。

参考文献

［1］「情報セキュリティポリシーに関するガイドライン」(平成 12 年 7 月 18 日：情報セキュリティ対策推進会議決定)

［2］BS7799 Information security management(英国規格協会)

Part1:Code of practice for information security management(1999 年)

Part2:Specification for information security management systems(1999 年)

［3］ISO/IEC TR 13335 Guidelines for the management of IT Security(国際標準化機構)

Part1:Concepts and models for IT Security(1996 年)

Part2:Managing and planning IT Security (1997 年)

Part3:Techniques for the management of IT Security(1998 年)

Par 4:Selection of safeguards(2000 年)

［4］ISO/IEC 15408 Evaluation criteria for IT security(国際標準化機構)

Part 1: Introduction and general model(1999 年)

Part 2: Security functional requirements (1999 年)

Part 3: Security assurance requirements (1999 年)

［5］金融機関等におけるセキュリティポリシー策定のための手引書(平成 11 年 1 月・財団法人金融情報システムセンター)

［6］情報システム安全対策基準(平成 7 年・通商産業省告示)

［7］コンピュータ不正アクセス対策基準(平成 8 年・通商産業省告示)

［8］コンピュータウイルス対策基準(平成 7 年・通商産業省告示)

［9］ソフトウェア管理ガイドライン(平成 7 年・通商産業省策定)

［10］システム監査基準(平成 8 年・通商産業省公表)

［11］行政情報システムの安全対策指針(平成 11 年 7 月 30 日・行政情報システム各省庁連絡会議幹事会了承)

［12］情報システム安全対策指針(平成 9 年・国家公安委員会告示)

［13］国家公務員法

［14］地方公務員法

［15］個人情報保護基本法制に関する大綱(平成 12 年 10 月 11 日・情報通信技術戦略本部)

［16］JIS Q 15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」(平成 11 年 4 月・財団法人日本規格協会)

［17］不正アクセスの禁止等に関する法律

［18］行政機関の保有する情報の公開に関する法律

［19］著作権法

［20］大東市電子計算組織および情報システム管理運用規程

［21］金沢市電子計算機処理データ保護管理規程

［22］高知市電子計算機処理情報管理規程

［23］新潟市電子計算機処理管理運営規程

［24］宗像市戸籍情報システムに係るデータ保護管理規程

［25］宗像市電子計算組織の管理、運営に関する規程

［26］新潟市電子計算機処理に係る個人情報の保護に関する条例

［27］新潟市電子計算機処理に係る個人情報の保護に関する条例施行規則

［28］KBMS-3 リファレンスマニュアル, NTT ソフトウェア

［29］KBMS-3 ユーザマニュアル NTT ソフトウェア